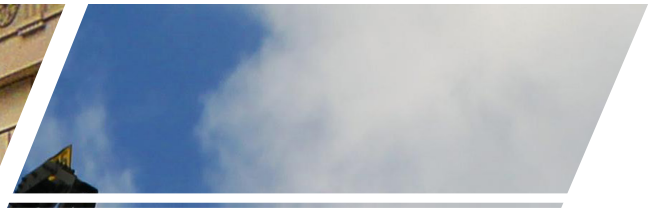
UIMCert® GmbH

Unternehmens- und Informations-Management Certification

UIMCert GmbH + Otto-Hausmann-Ring 113 + 42115 Wuppertal + Tel: (0202) 9467 726-300 + Fax: (0202) 9467 726-9300 + Mail: certification@uimcert.de + Internet: www.UIMCert.de

Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme

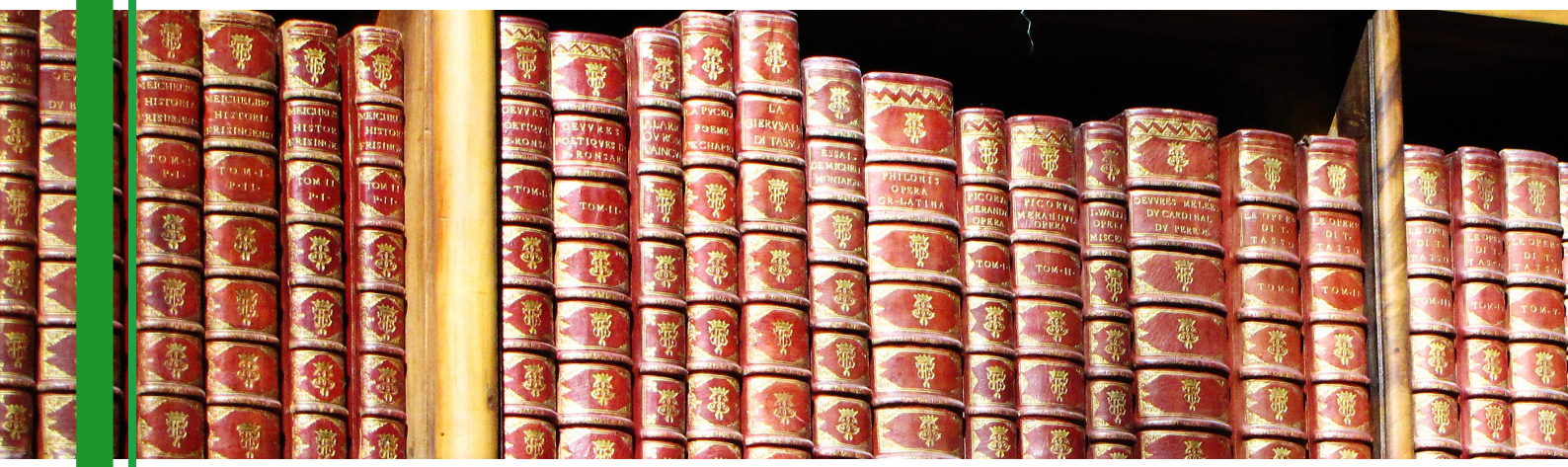
(IT-Sicherheitsgesetz / IT-SiG)



akkreditiert bei DAkkS Deutsche Akkreditierungsstelle D-ZM-17294-01-01

UIMCert GmbH
Otto-Hausmann-Ring 113
42115 Wuppertal
Tel: (0202) 9467 726-300
Fax: (0202) 9467 726-9300
E-Mail: certification@uimcert.de
Internet: www.UIMCert.de

UIMCert® GmbH



Was ist das IT-Sicherheitsgesetz?

Das IT-Sicherheitsgesetz ist ein „Artikelgesetz“, d.h. es beschränkt sich auf die Änderung bestehender Gesetze. Zentral ist die Änderung des BSI-Gesetzes; aber auch im Energiewirtschafts- und Telekommunikationsgesetz sind Änderungen herbeigeführt worden. So ist neben dem BSI bspw. auch die Bundesnetzagentur eine Aufsichtsbehörde über die Betreiber von „kritischen Infrastrukturen“, kurz KRITIS. Hierzu zählen Einrichtungen aus dem Bereich der Versorgung mit Grundbedürfnissen (Energie, Wasser, Ernährung, Gesundheit), sowie den Sektoren Finanz- und Versicherungswesen, Transport, Informationstechnik und Telekommunikation, soweit sie „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind“. Im Vergleich der genannten Branchen zeigte sich bisher ein uneinheitliches IT-Sicherheitsniveau, was auch auf die bis dato fehlenden branchenübergreifenden Regelungen zurückzuführen ist.

Das IT-Sicherheitsgesetz (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) hat zum Ziel, die IT-Sicherheit insbesondere bei Institutionen innerhalb der kritischen Infrastrukturen („KRITIS“) gesetzlich zu regeln und zu verbessern. Unternehmen müssen nun gewisse Mindestanforderungen erfüllen und diese auch nachweisen. Die Institutionen sind ferner verpflichtet, Hackerangriffe an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden.

Durch das IT-Sicherheitsgesetz wurden außerdem weitere Gesetze wie z. B. das Energiewirtschaftsgesetz geändert. Durch die Änderung des Energiewirtschaftsgesetz werden sämtliche Strom- und Gasnetzbetreiber verpflichtet, den IT-Sicherheitskatalog der Bundesnetzagentur umzusetzen und ein ISMS einzuführen.

Muss mein Unternehmen das Gesetz einhalten?

Das IT-Sicherheitsgesetz enthält Anforderungen an die Informationssicherheit zum Schutz kritischer Infrastrukturen. Demnach müssen „nur“ Unternehmen das IT-Sicherheitsgesetz beachten, welche in diesem Bereich tätig sind. Der Begriff „Kritische Infrastruktur“ (KRITIS) wurde vom Bundesministerium des Innern wie folgt definiert:

> „Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“

Die KRITIS wurden in folgende Sektoren aufgeteilt:

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Staat und Verwaltung
- Medien und Kultur

Sofern Sie unsicher sind, ob Ihr Unternehmen ebenfalls in diese Sektoren fällt, können Sie gerne auf uns zukommen.

Wissenswertes zum IT-Sicherheitsgesetz

Was muss in unserem Unternehmen beachtet und umgesetzt werden?

Das IT-Sicherheitsgesetz verlangt von KRITIS-Betreibern, unter Einhaltung des aktuellen Stands der Technik, die Implementierung von organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse.

Zusätzlich wird eine Überprüfung der Umsetzung der im IT-Sicherheitsgesetz festlegten Anforderungen gefordert. Diese Überprüfung soll alle zwei Jahre stattfinden und kann sowohl durch Zweitparteienaudits oder insbesondere durch eine branchenübliche Zertifizierung nachgewiesen werden. Die für die jeweiligen Branchen relevanten Standards und Verfahren können vom BSI unter Berücksichtigung der Betreiber und der Wirtschaftsverbände definiert werden.

Müssen wir uns an einer ISO-Norm orientieren?

Für Betreiber von Energieversorgungsnetzen und Energieanlagen wurde von der Bundesnetzagentur (BNetzA) im Benehmen mit dem BSI ein Sicherheitskatalog erstellt, nach dessen Vorgaben sich die Betreiber auszurichten haben.

Die BNetzA hat hierzu den IT-Sicherheitskatalog entwickelt und veröffentlicht, welcher die Einführung und Umsetzung eines Informationssicherheitsmanagementsystems (ISMS) für die IKT-Systeme der Netzbetreiber fordert. Innerhalb dieses Katalogs wird auf den Informationssicherheitsmanagementstandard ISO/IEC 27001 in Verbindung mit branchenspezifischen Sub-Normen verwiesen.

Das ISMS soll auf Basis der ISO/IEC 27001 geplant und implementiert werden. Bei der Implementierung sind hierbei die Anforderungen der ISO 27002 sowie der jeweiligen branchenspezifischen Subnormen (bspw. DIN ISO/IEC TR 27019 „Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung“) zu berücksichtigen. Innerhalb der ISO 27002 und den darauf aufbauenden Subnormen werden Hilfen bei der Umsetzung der ISMS Anforderungen gegeben und die Standardmaßnahmen um die branchentypischen Sicherheitsbelange erweitert.

Telekommunikationsdiensteanbieter, Betreiber von öffentlichen Telekommunikationsnetzen und Erbringer von öffentlich zugänglichen Telekommunikationsdiensten müssen sich den Anforderungen des „Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten“ unterwerfen. Hierbei wird ebenfalls auf die ISO 27001 als Grundlage für den Aufbau eines ISMS referenziert.

Welche Meldepflichten bestehen?

Betreiber kritischer Infrastrukturen müssen eine Kontaktstelle einrichten, um Informationen durch das BSI zu erhalten und erhebliche Störungen der Verfügbarkeit, Vertraulichkeit, Integrität oder Authentizität an das BSI zu melden. Eine Ausnahme hiervon bilden die Bereiche Energie und Telekommunikation, welche zwar ebenfalls einen Ansprechpartner für IT-sicherheitsrelevante Themen benennen müssen, die Meldungen aber an die Bundesnetzagentur erfolgen.

> Betreiber von Strom- und Gasnetzen mussten der BNetzA bis zum 30.11.2015 einen Ansprechpartner IT-Sicherheit benennen.

Ist eine Zertifizierung verpfichtend?

Eine Kernvorgabe des IT-Sicherheitsgesetzes ist die Forderung, dass Betreiber kritischer Infrastrukturen „angemessene technische und organisatorische Vorkehrungen zur Vermeidung von Störungen“ treffen und dabei den Stand der Technik einhalten müssen. Als „angemessene Vorkehrungen“ wird der Aufbau eines ISMS und die Ausrichtung nach dem Informationssicherheitsstandard ISO 27001 gemeinhin angesehen. Das IT-Sicherheitsgesetz fordert weiterhin, dass die Umsetzung der technischen und organisatorischen Maßnahmen durch Audits oder Zertifizierungen nachgewiesen wird. Ein solcher Nachweis kann durch eine ISO 27001 Zertifizierung erbracht werden.

Für Betreiber von Energienetzen ergibt sich die Forderung nach einer Zertifizierung durch den IT-Sicherheitskatalog. Dort wird explizit eine Zertifizierung des ISMS gemäß ISO 27001 durch eine akkreditierte Zertifizierungsstelle (wie z. B. die UIMCert) gefordert. Diese Zertifizierung muss durch die betroffenen Strom- und Gasnetzbetreiber bis zum 31.01.2018 nachgewiesen werden.

UIMCert® GmbH

Ablauf einer Zertifizierung gemäß ISO 27001

1. Stufe-1-Audit

- Dokumentationsprüfung
- Ggf. Übersendung der Auditfeststellungen an den Kunden
- Grundlegende Feststellung zur Zertifizierungsfähigkeit

2. Stufe-2-Audit

- Auditierung der Ergebnisse der Dokumentenprüfung vor Ort
- Erstellung des Auditberichts

3. Entscheidung über Zertifikatsvergabe

Die oben dargestellten Schritte stellen den Auditierungs-/Zertifizierungsablauf dar. Dieser besteht aus drei Teilen. **Im Stufe-1-Audit** findet eine grundsätzliche Betrachtung des Managementsystems auf Basis der Dokumentation als Vorbereitung auf das Stufe-2-Audit dar. Zusätzlich muss zur Bewertung der grundsätzlichen Zertifizierungsfähigkeit des Informationssicherheitsmanagementsystems eine Vor-Ort-Begehung erfolgen. Die Norm sieht vor, dass nach Stufe 1 ein Abbruch des Audits möglich ist, sollte die Dokumentation und/oder andere individuelle Bedingungen dies nahelegen. Auditfeststellungen aus der Stufe 1 werden dokumentiert und Ihnen mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten.

Die **Stufe 2** beinhaltet das eigentliche Audit in Form eines Vor-Ort-Audits. Hierbei wird die Umsetzung einschließlich der Wirksamkeit des Managementsystems des Kunden unter Berücksichtigung der verschiedenen Standorte bewertet. Auf Basis des abschließenden Prüfberichts wird dann durch die Zertifizierungsstellenleitung die Entscheidung über die Erteilung bzw. Verlängerung des Zertifikats getroffen.

Unterstützungsmöglichkeiten durch die UIMCert

Erstzertifizierungs-Audit

Voraussetzungen

Die UIMCert darf kein ISMS zertifizieren bevor der Auditee nicht mindestens ein Management Review und ein internes Audit durchgeführt hat. Der Auditee muss ein zertifizierungsnormkonformes, dokumentiertes und implementiertes ISMS betreiben. Die UIMCert darf keine bestimmte Art der Dokumentation des ISMS voraussetzen. Das Erstzertifizierungsaudit setzt sich aus zwei Stufen zusammen.

Stufe 1

In der ersten Auditstufe werden folgende Themen begutachtet:

- Auditierung der Managementsystem-Dokumentation
- Beurteilung der standortspezifischen Bedingungen
- Ermittlung der Bereitschaft für ein Stufe-2 Audit
- Bewertung des Status im Hinblick auf das Verständnis der Normanforderungen, die Identifizierung von Schlüsselleistungen und das Betreiben des ISMS
- Sammlung von Informationen bzgl. des Geltungsbereichs, der Standorte und der zugehörigen gesetzlichen und regulatorischen Aspekte und deren Einhaltung
- Bewertung der Zuteilung der Ressourcen für Stufe-2 Audit
- Bestimmung der Schwerpunkte für das Stufe-2 Audit
- Beurteilung, ob interne Audits und Managementbewertungen geplant und durchgeführt werden.

Dabei geht es in erster Linie darum sich einen Eindruck über die Zertifizierungsreife der jeweiligen Organisation zu verschaffen und aus diesen gewonnenen Informationen nähere Einzelheiten für den zweiten Schritt des Audits zu ermitteln, so dass sich die zweite Phase des Audits und die eingesetzten Ressourcen planen lassen.

Weiterhin werden die Ergebnisse dem Auditee in Form eines schriftlichen Berichts zur Verfügung gestellt und dienen ihm zur Umsetzung der zur Normerfüllung notwendigen Änderungen im Unternehmen. Dabei wird der Auditee auf Findings hingewiesen, die innerhalb des Stufe-2 Audits als Nichtkonformitäten gewertet werden könnten.

Je nach Art und Umfang der im Stufe-1 Audit aufgedeckten Sachverhalte und ggfs. erkannten Findings wird entschieden, ob der Auditee für das Audit der Stufe 2 bereit ist und ob das Stufe-2 Audit sinnvoll durchgeführt werden kann. In Abhängigkeit dieser Ergebnisse wird ein Termin für das Stufe-2 Audit vereinbart.

Stufe 2

Im zweiten Schritt wird die Umsetzung der Normforderungen vor Ort begutachtet und bewertet. Am Abschluss der beiden Phasen des Audits wird vom Auditteam ein Auditbericht erstellt, welcher später als Grundlage für die Zertifizierungsentscheidung dient.

Folgende Informationen müssen die Auditoren der Leitung der Zertifizierungsstelle zur Verfügung stellen, damit diese eine Entscheidung über die Zertifizierung treffen kann:

- Auditberichte
- Anmerkungen zu den Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die von der auditierten Organisation getroffen wurden,
- Bestätigung der an die Zertifizierungsstelle gelieferten Informationen, die in der Antragsprüfung verwendet wurden und
- Empfehlung, ob die Zertifizierung gewährt werden soll (zusammen mit Bedingungen bzw. Beobachtungen).

Überwachungsaudits (periodische Audits)

Zur Überprüfung der Normkonformität finden Überwachungsaudits bei den zertifizierten Organisationen statt. Die Audits sollen mit Ausnahme des Rezertifizierungsaudits je innerhalb eines Kalenderjahres stattfinden, das erste Überwachungsaudit jedoch innerhalb der ersten 12 Monate nach dem Zertifizierungsaudit. Das Überwachungsaudit stellt ein Vor-Ort-Audit dar, bei dem

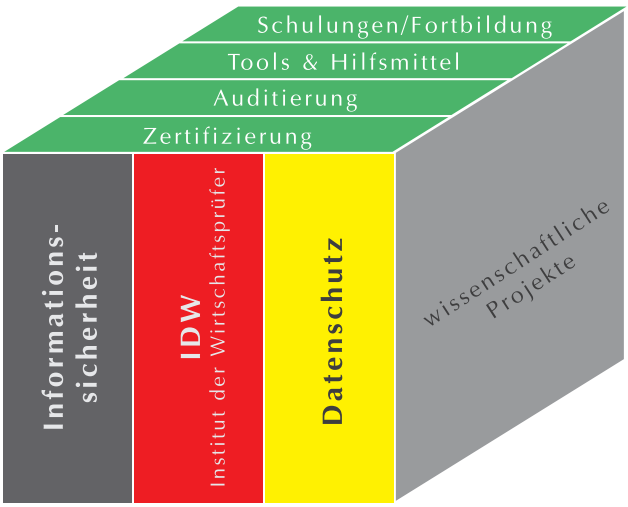
- die zur Beseitigung der Schwachstellen ergriffenen Maßnahmen bewertet werden.
- eventuelle Beschwerden behandelt werden.
- die Wirksamkeit des Managementsystems überprüft wird.
- festgestellt wird, ob die Fortschritte geplanter Tätigkeiten auf eine ständige Verbesserung abzielen.
- Änderungen, die dem ISMS unterliegen, Änderungendes SoA oder von umgesetzten Maßnahmen bewertet werden.
- die Implementierung, Aufrechterhaltung und Effektivität von Maßnahmen geprüft werden.
- die ordnungsgemäße Nutzung von Zeichen und Zertifizierungsverweisen geprüft wird
- die Risikobetrachtung überwacht wird.
- interne Audits, die Managementbewertung und korrektive Maßnahmen überwacht werden.

UIMCert® GmbH

Informationssicherheits- und Informationsmanagement

Die Informationsmanagementsysteme werden nach den Anforderungen der Informationssicherheitsmanagement-Norm ISO 27001 hinsichtlich der organisatorischen Grundlagen der Informationssicherheit und deren Umsetzung geprüft. Hierbei kann die Umsetzung der geforderten Informationssicherheitsaspekte ebenso betrachtet werden wie ergänzend die Anforderungen des BDSG.

Eine Zertifizierung gemäß **ISO 27001** (nativ oder auf Basis des IT-Grundschutzes des BSI) basiert auf vorgegebenen Verfahren und Abläufen im Hinblick auf einen spezifischen Anforderungskatalog. Daneben bieten wir Ihnen auch die Möglichkeit, ausgewählte Gebiete der IT-Sicherheit zu auditieren. Ergänzend hierzu können **ITIL-orientierte Prüfungen** auf Basis der ISO 20000 für Prozesse und Verfahren des Servicemanagements durchgeführt werden.



Datenschutz

Die **Prüfungsstandardreihe der UIMCert** „ Standards für die Prüfung der Datenschutzordnungsmäßigkeit von verarbeitenden/verantwortlichen Stellen (PS 101)“, „Produkten/Systemen (PS 102)“ und „Verfahren (PS 103)“ zeigt die Anforderungen der Datenschutzordnungsmäßigkeit auf. Die Prüfungshandlungen beziehen sich primär auf die gelebte Umsetzung der Anforderungen.

In vielen Datenschutzgesetzen ist eine **Vorabkontrolle** gefordert. So müssen automatisierte Datenverarbeitungsverfahren (IT-Programme/-Systeme) noch vor der Einführung auf ihre Ordnungsmäßigkeit geprüft werden. Auch wenn dies oftmals zu den originären Aufgaben des DSB gehört, kann die UIMCert vorbereitend unterstützen. Gleiches gilt auch für die gemäß EU-Datenschutz-Grundverordnung für Verfahren vorgesehene **Datenschutz-Folgeabschätzung**, welche nach dem 25.05.2018 in Betrieb genommen werden.

Wir können die Umsetzung der vertraglich vereinbarten Sicherheits- und Datenschutzmaßnahmen durch die Kunden bei den Dienstleistern gemäß den Anforderungen zur **Auftragsdatenverarbeitung** überprüfen, auch innerhalb eines Vor-Ort-Audittermins (sämtliche Rechtsnormen).

Ferner kann eine Datenschutz-Gütesiegelung durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), das erste staatliche **Gütesiegel** im Datenschutzbereich, für IT-Produkte vorgenommen werden. Ein wesentlicher Bestandteil der Prüfung, die wir im Rahmen unserer Tätigkeiten als sachverständige Prüfstelle durchführen, ist die Dokumentation des Produkts/Verfahrens.

UIMCert: Ihr Zertifizierer

Die UIMCert GmbH ist ein führendes Unternehmen in den Bereichen IT-Sicherheits- und Datenschutzzertifizierung. Wir haben einen unabhängigen Ausschuss zur Sicherstellung der Unparteilichkeit, der die Geschäftsführung in wichtigen Fragen im Bereich IT-Management, IT-Sicherheit und Datenschutz sowie Zertifizierung berät.

Wir verfügen über qualifiziertes und erfahrenes Personal für die Auditierung und Zertifizierung in den genannten Bereichen. Wir sind bei der „Deutschen Akkreditierungsstelle GmbH“ (**DAkkS**) für den Standard ISO 27001 und Prototypenschutz sowie beim „Unabhängiges Landeszentrum für den Datenschutz“ (**ULD**) für Datenschutzauditierung (für Recht und Technik) akkreditiert.

Wir haben darüber hinaus eigene Prüfsysteme für IT-Sicherheit und Datenschutz (datenverarbeitende Stellen und Produkte) entwickelt, innerhalb derer wir nach erfolgreicher Auditierung gemäß prüfbaren standardisierten Normen ein **eingetragenes Gütesiegel** verleihen.

Informationssicherheit

- ISO 27001 (nativ)
- ISO 27001 auf Basis IT-Grundschutz
- Umsetzung des Best Practice ISO 27002
- interne Audits /Analysen (SiSSA)

Informationsmanagement

- ISO 20000 (Service-Management)
- Auswahl und Prüfung einzelner Bausteine

Institut der Wirtschaftsprüfer IDW

- IDW PS 330 (Sicherheitsaudit)
- IDW PS 331 (Sicherheitsaudit)
- IDW PS 880 (Software)

Datenschutz

- ULD-Gütesiegel
- UIMCert-Gütesiegel [Stellen, Produkte und Verfahren]
- Audit im Rahmen der Auftragsdatenverarbeitung
- Vorabkontrollen
- interne Audits /Analysen (Datenschutz-Checkup)

Grundsätzlich sind Prüfungen auf Basis aller Datenschutzgesetze möglich (Bundes-, Landes-, Kirchen- und Sozialrecht)

Normen der Wirtschaftsprüfer/ IDW-Standards

Rechnungsrelevante Verfahren und Produkte müssen auf ihre **Ordnungsmäßigkeit** geprüft werden. Hierbei bietet die UIMCert die Erstellung von Testaten auf Grundlage der Standards des **Instituts der Wirtschaftsprüfer** (IDW) an, die insbesondere für Hersteller und Anbieter von entsprechenden Systemen, aber auch für die einsetzenden Institutionen von hohem Nutzen sind.

Schulung, Fortbildung, Tools und wissenschaftliche Projekte

Wir führen auch **wissenschaftliche Projekte** durch, vor allem auf den Gebieten E-Business und IT-Sicherheit. Auch bieten wir **Workshops** für Führungskräfte, Schulungen für Mitarbeiter sowie Aus-, Fort- und Weiterbildungsmaßnahmen für Fachkräfte in der IT-Sicherheit und im Datenschutz als UIMCollege-**Seminar** oder als Inhouse-Veranstaltung an. Ferner kann mittels eCollege unabhängig von Ort und Zeit Wissen vermittelt und Mitarbeiter sensibilisiert werden.

Durch die Verbindung mit der UIMC stehen der UIMCert die von der UIMC entwickelten **Tools** zur Verfügung, die eine hohe Effizienz durch computerisiertes Arbeiten ermöglichen, wie z. B. das UIMC-Tool für Analyse und Berichterstellung (UTAB).

UIMCert® GmbH

Umsetzung des IT-Sicherheitsgesetzes mit Hilfe der UIMCert

Wie kann uns die UIMCert unterstützen?

Als akkreditiertes Unternehmen können wir Ihnen folgende Unterstützung anbieten:

- Auditierung der Managementsystem-Dokumentation
- Beurteilung der standortspezifischen Bedingungen
- Ermittlung der Bereitschaft für Zertifizierungsaudit
- Begutachtung der Umsetzung der Normforderungen vor Ort
- Begutachtung der Umsetzung der dokumentierten Verfahren
- Überprüfung der Leistungsfähigkeit des ISMS

Wenn die Institution nicht weiß, wo Sie qualitativ steht, hat die UIMCert ein Konzept entwickelt, um den Status quo der Institution zu evaluieren. Die UIMCert kann:

- Prüfung des Fortschritts der Implementierung eines ISMS
- Ermittlung des Grades der Erfüllung anwendbarer Anforderungen an das ISMS
- Prüfung der Anwendung und Wirksamkeit des ISMS
- Identifikation von Sicherheitsschwachstellen
- Feststellung von Verbesserungspotential

Zu Beginn kann auch gerne zunächst ein Workshop durchgeführt werden, durch den das Projekt, die ausgewählten Normen und die Ziele definiert werden können.

Warum sollte uns gerade die UIMCert unterstützen?

Die UIMCert besitzt als DAkkS akkreditiertes Unternehmen umfangreiche fachliche Kompetenz im Umfeld der Informationssicherheit. Durch unsere qualifizierten ISO 27001 Lead-Auditoren, Auditteamleiter und Datenschutzexperten, die sowohl mit Zertifizierungen und Gütesiegelungen als auch mit Normen und deren Eigenheiten bestens vertraut sind und damit ausführliche Fach- und Methodenkompetenz besitzen, können wir Ihnen praxisgerechte Auditierungen bieten und Sie auf dem Weg zur Zertifizierung unterstützen.

Die UIMCert kennt die Informationssicherheitsmanagementprozesse in Institutionen unterschiedlicher Branchen sehr genau und kennt daher auch die Fallstricke bei den jeweiligen Prozessen und kann gezielt auf die individuelle Situation der Auditees eingehen.

Die UIMCert bietet die Durchführung von Prüfungshandlungen zur Erlangung eines ISO 27001 Zertifikats, bei Bedarf unter Berücksichtigung von branchenspezifischen Subnormen, sodass der Beleg für die Umsetzung der Forderungen des IT-Sicherheitsgesetzes eine hohe Glaubwürdigkeit und damit hohe Akzeptanz aufweist.

Durch die jahrelange Tätigkeit in diesem Normumfeld und durch Festlegung der genauen Arbeitsschritte können wir mit Ihnen gemeinsam ein klar strukturiertes und transparentes Verfahren durchführen und helfen Ihnen somit, Zeit und damit auch Kosten zu sparen. Die Ergebnisse der Begutachtung werden von uns in einem Bericht zusammengefasst, mit welchem Sie durch die Dokumentation der eventuellen Auditfindings auch gleichzeitig eine Möglichkeit zur Optimierung Ihres ISMS erhalten.

Gerne können wir Ihnen unsere Unterstützung vollkommen unverbindlich einmal persönlich vorstellen. Wir freuen uns auf Ihren Kontakt.

Welche Vorteile und Nutzen bringt die UIMCert-Unterstützung?

- Fach- und Methodenkompetenz im Fachgebiet und in der Ordnungsmäßigkeitsprüfung
- unabhängige, schnelle und routinierte Prüfung von Verfahren und Konzepten
- Nutzung eines etablierten Tools zur Effizienz- und Effektivitätssteigerung
- langjährige Erfahrungen in der Auditierung und Zertifizierung
- Rückgriff auf Best-Practice-Lösungen und -Vorgehensweisen
- hohe Qualität durch langfährig festangestellte, eigene Auditoren

Fragen?
Interesse?

Dann zögern Sie nicht und sprechen uns an:

(0202) 9467 726-300
certification@uimcert.de